



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,297	12/31/2003	Richard M. Shupak	MSFT-2568/307781.01	1690
41505	7590	09/28/2007	EXAMINER	
WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)			SCHMIDT, KARL	
CIRA CENTRE, 12TH FLOOR			ART UNIT	PAPER NUMBER
2929 ARCH STREET			2139	
PHILADELPHIA, PA 19104-2891			MAIL DATE	DELIVERY MODE
			09/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	10/750,297	SHUPAK ET AL.
	Examiner Kari L. Schmidt	Art Unit 2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 09 July 2007.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-27 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-27 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 31 December 2003 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date _____.
 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date _____.
 5) Notice of Informal Patent Application
 6) Other: _____.

DETAILED ACTION

Notice to Applicant

This communication is in response to the amendment filed on 07/09/2007.

Claims 1-27 remain pending. Claim 10 has been amended.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 11-18 recites the limitation "the computer readable medium" in the following claims. There is insufficient antecedent basis for this limitation in the claim. The examiner will interpret this to be the "tangible computer readable medium" as in the independent claim 10.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-27 are rejected under 35 U.S.C. 102(b) as being anticipated by Richarte, Gerardo. "Four different tricks to bypass StackShield and StackGuard protection".

Claim 1

Richarte discloses a method of processing runtime functions, comprising: receiving a call to a runtime function; determining associated data from the call to the runtime function; determining a target from the associated data; and executing the target (see at least, Section 2).

Claim 2

Richarte discloses the method of claim 1, wherein the step of determining the associated data comprises accessing data in a data structure connected with the runtime function and calculating the associated data based on the accessed data (Section 2.3).

Claim 3

Richarte discloses the method of claim 1, further comprising:
determining if at least a portion of the associated data is valid; and preventing execution
of the target if the associated data is not valid (see at least, Section 2.3 and page 8).

Claim 4

Richarte discloses the method of claim 3, further comprising maintaining a list of valid
targets, wherein the step of determining if the associated data is valid comprises
comparing the target to the list of valid targets (see at least, Section 2.3).

Claim 5

Richarte discloses the method of claim 4, wherein maintaining the list comprises
generating the list of valid targets at compiler and link time (see at least, Section 2.3.4
and page 9).

Claim 6

Richarte discloses the method of claim 4, wherein maintaining the list comprises
generating the list of valid targets at runtime (see at least, Section 2.3 and page 6).

Claim 7

Richarte discloses the method of claim 3, wherein the step of determining if the
associated data is valid comprises retrieving a security cookie from the associated data

and comparing the retrieved security cookie to a list of valid security cookies (see at least, page 10-11 and Section 2.5.1: canary = security cookie and page 28).

Claim 8

Richarte discloses the method of claim 3, further comprising determining and storing a predetermined calculated value based on at least a portion of the associated data, prior to receiving the call to the runtime function (see at least, Section 3).

Claim 9

Richarte discloses the method of claim 8, wherein determining if the associated data is valid comprises comparing the predetermined calculated value to another calculated value based on the associated data (see at least, Section 3).

Claim 10

Richarte discloses a tangible computer-readable medium having stored thereon computer-executable instructions for performing a method of processing runtime functions, the method comprising: receiving a call to a runtime function; determining associated data from the call to the runtime function; determining a target from the associated data; and executing the target (see at least, Section 2).

Claim 11

Richarte discloses the computer readable medium of claim 10, wherein the step of determining the associated data comprises accessing data in a data structure connected with the runtime function and calculating the associated data based on the accessed data (see at least, Section 2.3).

Claim 12

Richarte discloses the computer readable medium of claim 10, having further computer-executable instructions for determining if at least a portion of the associated data is valid, and preventing execution of the target if the associated data is not valid (see at least, Section 2.3 and page 8).

Claim 13

Richarte discloses the computer-readable medium of claim 12, having further computer-executable instructions for maintaining a list of valid targets, wherein the step of determining if the associated data is valid comprises comparing the target to the list of valid targets (see at least, Section 2.3).

Claim 14

Richarte discloses the computer-readable medium of claim 13, wherein maintaining the list comprises generating the list of valid targets at compiler and link time (see at least, Section 2.3.4 and page 9).

Claim 15

Richarte discloses the computer-readable medium of claim 13, wherein maintaining the list comprises generating the list of valid targets at runtime (see at least, Section 2.3 and page 6).

Claim 16

Richarte discloses the computer-readable medium of claim 12, wherein determining if the associated data is valid comprises retrieving a security cookie from the associated data and comparing the retrieved security cookie to a list of valid security cookies (see at least, page 10-11 and Section 2.5.1: canary = security cookie and page 28).

Claim 17

Richarte discloses the computer-readable medium of claim 12, having further computer-executable instructions for determining and storing a predetermined calculated value based on at least a portion of the associated data, prior to receiving the call to the runtime function (see at least, Section 3).

Claim 18

Richarte discloses the computer-readable medium of claim 17, wherein determining if the associated data is valid comprises comparing the predetermined calculated value to another calculated value based on the associated data (see at least, Section 3).

Claim 19

Richarte discloses a system for processing runtime functions, comprising: a processor that receives a call to a runtime function; and a dispatcher system (see at least, Section 2: "StackGuard") that determines associated data from the call to the runtime function, determines a target from the associated data, and executes the target (see at least, Section 2).

Claim 20

Richarte discloses the system of claim 19, wherein the dispatcher system comprises a module to access data in a data structure connected with the runtime function and calculate the associated data based on the accessed data (see at least, Section 2.3).

Claim 21

Richarte discloses the system of claim 19, wherein the dispatcher system comprises modules to determine if at least a portion of the associated data is valid and prevent execution of the target if the associated data is not valid (see at least, Section 2.3 and page 8).

Claim 22

Richarte discloses the system of claim 21, further comprising a storage device that stores a list of valid targets, wherein the dispatcher system determines if the associated

data is valid by comparing the target to the list of valid targets (see at least, Section 2.3).

Claim 23

Richarte discloses the system of claim 22, further comprising a compiler that generates the list of valid targets (see at least, Section 2.3).

Claim 24

Richarte discloses the system of claim 21, wherein the dispatcher system determines if the associated data is valid by retrieving a security cookie from the associated data and comparing the retrieved security cookie to a list of valid security cookies (see at least, page 10-11 and Section 2.5.1: canary = security cookie and page 28).

Claim 25

Richarte discloses the system of claim 21, wherein the processor determines and stores a predetermined calculated value based on at least a portion of the associated data, prior to receiving the call to the runtime function (see at least, Section 3).

Claim 26

Richarte discloses the system of claim 25, wherein the dispatcher system determines if the associated data is valid by comparing the predetermined calculated value to another

calculated value based on the associated data (see at least, Section 3).

Claim 27

Richarte discloses the system of claim 19, further comprising a compiler and a linker that compiles code to produce an executable that is marked with an identifier indicating that the executable supports runtime protection (see at least, page 9 and pages 19-20).

Response to Arguments

Applicant's arguments filed 09-July-2007 have been fully considered but they are not persuasive.

With respect to independent claim 1, the applicant argues that Richarte, Gerardo fails to describe or suggest **determining associated data from a call to a runtime function or determining a target from associated data**. The examiner respectively disagrees with this argument.

With respect to the argument, the examiner notes that Richarte, Gerardo does indeed teach **determining associated data from a call to a runtime function or determining a target from associated data**. Claim 1 is any function executed: receiving a call to a run time function (see at least, Section 2.1: "entry to a function (function_prologue); calls like move, push, subl...etc"); **determining associated data from a call to a runtime function** (see at least, Section 2.2, page 6: the parameters passed to the function (\$0x00aff0d; %esp,..etc)); **determining a target from**

associated data (see at least, Section 2.2, 2.3, 3.1: the memory location where it reside (pointer location): “frame pointer”, “function pointer”); and executing the target (see at least, page 4: “func() body is executed”; page 5: “ the StackGuarded func() is being executed: the data in the stack is being moved”).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

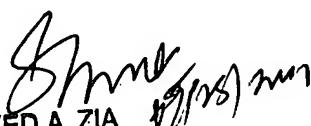
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kari L. Schmidt whose telephone number is 571-270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-270-2385.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KS


SYED A. ZIA
PRIMARY EXAMINER